# METHOD FOR PREPARING CIPHER ENVELOPE

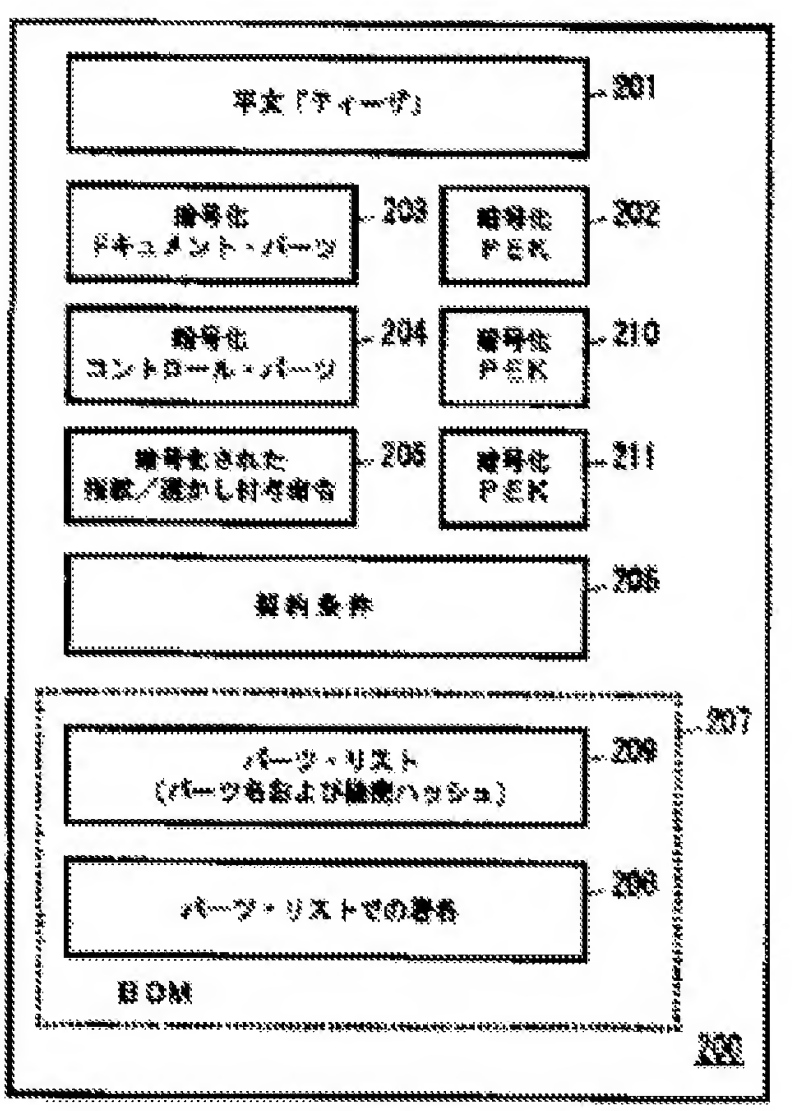
**Patent number:** JP10040100
**Publication date:** 1998-02-13
**Inventor:** AUERBACH JOSHUA SETH; CHOW CHEE-SENG; KAPLAN MARC ADAM; CRIGLER JEFFREY CHARLES
**Applicant:** IBM
**Classification:**
**- international:** ***G06F21/22; G06F9/06; G06F13/00; G06F21/00; G06Q10/00; G06Q30/00; G07F7/12; G09C1/00; H04L9/08; H04L9/14; H04L9/32;*** **G06F21/22; G06F9/06; G06F13/00; G06F21/00; G06Q10/00; G06Q30/00; G07F7/12; G09C1/00; H04L9/08; H04L9/14; H04L9/32;** (IPC1-7): G06F9/06; G06F13/00; G06F15/00; G06F17/60; G09C1/00; H04L9/08; H04L9/14
**- european:** G07F7/08E4; H04L9/32
**Application number:** JP19970071388 19970325
**Priority number(s):** US19960625475 19960329

**Also published as:**
EP0798892 (A2)
US5673316 (A1)
EP0798892 (A3)
EP0798892 (B1)
DE69736310T (T2)



Abstract of **JP10040100**

PROBLEM TO BE SOLVED: To obtain a method for preparing, distributing, and vending a digital document, and a method for managing access to the digital document by providing a step for enciphering one of information parts by a part enciphering key, and preparing an enciphered part to be housed in an envelope. SOLUTION: A document part 203 can be enciphered. The enciphered document part 203 can be a 'valuable content' (for example, the chapter of a book, high resolution JPEG picture, or MPEG stream) to be purchased by a user. A non-enciphered part is a 'thesis' (for example, a book review by the others, index, summarization, or low resolution JPEG picture). The purpose of the non-enciphered part is to allow the user to attain the 'preview', 'sampling' or 'browse' of the content of the enciphered envelope before actually purchasing it.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

**特開平10－40100**

(43)公開日　平成10年(1998)２月13日

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| Ｇ０６Ｆ | 9/06 | ５５０ | | Ｇ０６Ｆ | 9/06 | ５５０Ｚ |
| | 13/00 | ３５１ | | | 13/00 | ３５１Ｇ |
| | 15/00 | ３３０ | | | 15/00 | ３３０Ｚ |
| | 17/60 | | 7259－5Ｊ | Ｇ０９Ｃ | 1/00 | ６６０Ｅ |
| Ｇ０９Ｃ | 1/00 | ６６０ | | Ｇ０６Ｆ | 15/21 | Ｚ |

審査請求　未請求　請求項の数８　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平9－71388

(22)出願日　平成９年(1997)３月25日

(31)優先権主張番号　０８／６２５４７５

(32)優先日　1996年３月29日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

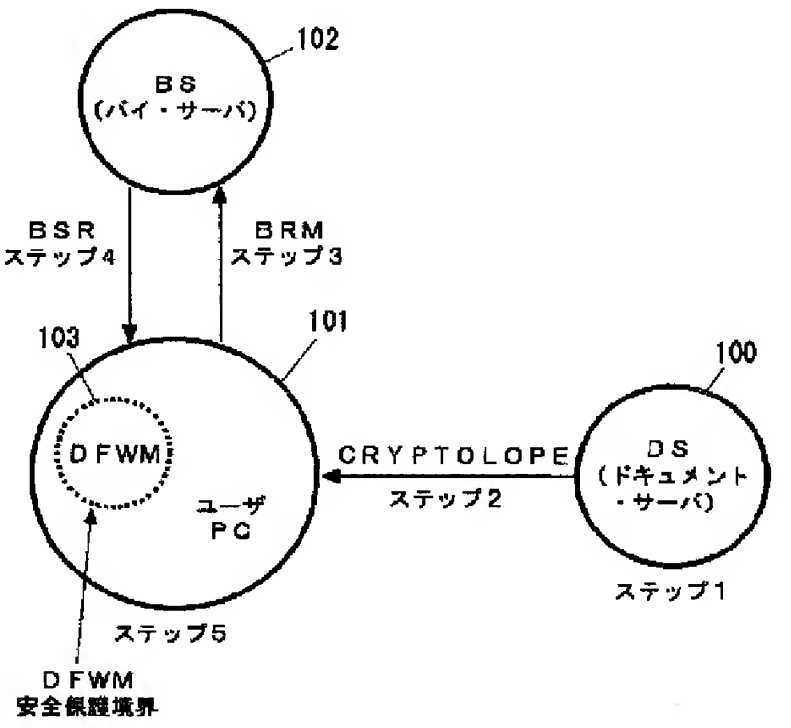
(72)発明者　ジョシュア・セス・オーバック
アメリカ合衆国06877　コネチカット州リッジフィールド　ホルムズ・ロード　129

(74)代理人　弁理士　合田　潔　（外２名）

最終頁に続く

(54)【発明の名称】　暗号エンベロープの作成方法

(57)【要約】
【課題】　安全な暗号エンベロープを使用して、ディジタル文書を作成し、配布し、販売し、アクセス管理を行う方法および装置。
【解決手段】　エンベロープは情報パーツの集合体であり、保護されるべきパーツの各々は対応するパーツ暗号化キーによって暗号化され、エンベロープの一部となる。各パーツ暗号化キーも公開キーによって暗号化され、エンベロープに収められる。エンベロープは各エントリがパーツ名と命名されたパーツの機密ハッシュを有しているパーツのリストも含んでいる。このリストは次いで、秘密キーによって署名されて、これもエンベロープに収められる署名を生成する。第１の秘密キーに関連づけられた第２の公開キーを使用して、署名を検証することができ、エンベロープ内の情報パーツの完全性は第２のハッシュを計算し、これをパーツのリストの対応するハッシュと比較することによって調べられる。



【特許請求の範囲】
【請求項１】複数のユーザに任意に配布でき、情報パーツの集合体であるディジタル文書である暗号エンベロープを作成する方法において、
ａ．前記情報パーツの１つをパーツ暗号化キーによって暗号化して、前記エンベロープに収められる暗号化パーツを作成するステップと、
ｂ．前記パーツ暗号化キーを第１の公開キーによって暗号化して、前記暗号エンベロープに収められる暗号化パーツ暗号化キーを作成するステップと、
ｃ．前記エンベロープに収められているパーツのリストであって、該リストの各エントリがパーツ名と該命名パーツの機密ハッシュとを含んでおり、該リストも前記エンベロープに収められるパーツのリストを作成するステップと、
ｄ．前記リストに第１の秘密キーによって署名して、前記エンベロープに収められる署名を作成するステップとを備えており、
前記リストの完全性を前記第１の秘密キーに関連づけられた第２の公開キーによって調べて、前記署名を検証することができ、前記エンベロープのいずれか１つのパーツの完全性を該１つのパーツの第２の機密ハッシュを計算し、かつ該第２のハッシュを前記リスト内の対応するハッシュと比較することによって調べることができ、前記暗号エンベロープの情報コンテンツが開示から保護され、前記パーツ暗号化キーによってのみ復元することができ、前記パーツ暗号化キーが前記第１の公開キーに対応する第２の秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読することによってのみ復元できる、
暗号エンベロープを作成する方法。
【請求項２】前記文書の前記パーツから選択したものを、この選択したパーツ内の選択したワードまたはビットの挿入、削除または変更により修正し、それぞれの未修正の文書を復元するために、修正した各ドキュメント・パーツをその修正に関連づける状態情報を維持するステップをさらに含んでいる、請求項１に記載の方法。
【請求項３】前記パーツの前記暗号化前に、前記修正を前記パーツから選択したものに適用し、第３の公開キーによって暗号化される第３のパーツ暗号化キーを使用して、前記状態情報を暗号化する、請求項２に記載の方法。
【請求項４】前記暗号エンベロープが、サーバで実行されるものであるコンピュータ・プログラムを含んでおり、前記実行の結果が前記サーバによる以降の操作を決定する、請求項１に記載の方法。
【請求項５】前記プログラムが前記暗号エンベロープ内の前記情報パーツのアクセスに関する契約条件を記述しており、前記実行が前記情報パーツへのアクセスが許可されるかどうかを決定する、請求項４に記載の方法。
【請求項６】前記プログラムが各情報パーツを修正する命令を含んでおり、各パーツが各パーツ内の選択したワードまたはビットの挿入、削除、または変更によって修正され、それぞれの未修正の文書を復元するために、修正した各ドキュメント・パーツをその修正に関連づける状態情報が維持される、請求項４に記載の方法。
【請求項７】暗号エンベロープ内のコンテンツ・データへのアクセスをもたらす方法において、
ａ．前記暗号エンベロープのパーツへのアクセス要求であり、前記パーツを暗号化するために使用されたキーの公開キー暗号化である暗号化パーツ暗号化キーを少なくとも含んでいる要求をユーザからのサーバに伝送するステップと、
ｂ．前記要求に応じて、前記サーバから前記ユーザへ、前記暗号化パーツ暗号化キーの変形物である応答を伝送するステップとを備えており、前記変形物が前記公開キーに関連づけられた秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読し、
第２の公開キーを使用して前記パーツ暗号化キーを暗号化し、
前記変形化キーを前記秘密キーを使用して、前記パーツ暗号化キーに暗号解読することによって生成され、前記の選択したパーツが前記パーツ暗号化キーを使用して平文テキストに暗号解読され、これによって前記ユーザにアクセスを与える前記方法。
【請求項８】複数の端末装置へ電子的にアクセスするサーバを有する通信ネットワークにおいて、選択したコンテンツ・データへのアクセスを与える方法において、前記暗号エンベロープが
ａ．複数のユーザに任意に配布でき、情報パーツの集合体であるディジタル文書である暗号エンベロープを作成することによって生成され、該生成方法が
（ｉ）その１つが前記の選択したコンテンツ・データを含んでいる、保護されるべき前記パーツの各々にパーツ暗号化キーを関連づけ、
（ｉｉ）保護されるべき前記パーツの各々をこれに関連したパーツ暗号化キーによって暗号化し、
（ｉｉｉ）前記の各パーツ暗号化キーを公開キーによって暗号化して、前記パーツ暗号化キーの各々に対する暗号化パーツ暗号化キーを形成し、
（ｉｖ）各エントリが前記パーツの１つに対するパーツ名と該１つのパーツに対する機密ハッシュとを含んでいるパーツのリストを作成し、
（ｖ）前記リストに秘密キーによって署名して、署名を作成することからなっており、前記暗号エンベロープが前記署名、前記リスト、前記暗号化パーツ暗号化キー、前記暗号化パーツ、および前記情報パーツのうち暗号化されていないものの集合体であり、
ｂ．前記暗号エンベロープのコピーを所有しているユーザが前記の選択したコンテンツ・データにアクセスすることを希望した場合に、

（ｉ）前記暗号エンベロープの前記の選択したコンテンツ・データを含んでいるパーツへのアクセス要求であり、前記パーツを暗号化するために使用されたキーの公開キー暗号化である暗号化パーツ暗号化キーを少なくとも含んでいる要求を前記ユーザからサーバへ伝送し、
（ｉｉ）前記要求に応じて、前記サーバから前記ユーザへ、前記暗号化パーツ暗号化キーの変形物である応答を伝送することによって前記アクセスが与えられ、前記変形物がステップｂ（ｉ）の前記公開キーに関連づけられた秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読し、
第２の公開キーを使用して前記要求の前記パーツ暗号化キーを暗号化し、
前記変形化キーを前記秘密キーを使用して、前記要求の前記パーツ暗号化キーに暗号解読することによって生成され、前記の選択したパーツが前記パーツ暗号化キーを使用して平文テキストに暗号解読され、これによって前記ユーザにアクセスを与える前記方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は安全な暗号エンベロープの方法および技法を使用したディジタル文書の作成、配布、および販売方法、ならびにディジタル文書へのアクセスの管理を記載する。

【０００２】

【従来の技術】ディジタル文書は紙ベースのアナログ文書を凌駕するさまざまな利点を有している。これらの文書は作成、配布および複製が容易である。しかしながら、これらの利点はこれらの文書に関連した知的所有権を侵害から守ることを困難とする。それにもかかわらず、ディジタル文書は将来の情報の配布および販売手段として紙ベースの文書に置き換わっていくであろう。

【０００３】

【発明が解決しようとする課題】
ＣＤ－Ｓｈｏｗｃａｓｅ（米国特許第５３１９７０５号）
本発明とＣＤ－Ｓｈｏｗｃａｓｅ特許［２］との重要な違いは、部分暗号キーが暗号エンベロープに収められており、公開キーで暗号化されるところにある。これに対し、ＣＤ－Ｓｈｏｗｃａｓｅでは、配布データが暗号キーの識別子を含んでいるだけである。暗号キーはサーバに記憶されており、キーの識別子が提示されたときに検索される。

【０００４】したがって、ＣＤ－Ｓｈｏｗｃａｓｅ特許では、キー・データベースをサーバに維持しておく必要があり、バイ・サーバとドキュメント・サーバとの間の信頼性に関する対策を必要とする。

【０００５】ＰＧＰ（Pretty Good Privacy）
ＰＧＰ［３］は安全な電子メールを送るための公開キー・ベースのシステムである。電子メールの本文はＩＤＥＡアルゴリズム（たとえば、［１］参照）を使用して暗号化され、暗号キーは予定している受信者の公開キーを使用して暗号化される。暗号化された電子メールのテキストと暗号化された暗号キーの両方が送られる。受信者は自分の秘密キーを使って、暗号キーを復元し、この暗号キーは平文のテキストを復元するために使用される。

【０００６】

【課題を解決するための手段】本発明は安全な暗号エンベロープの方法および技法を使用したディジタル文書の作成、配布、および販売方法、ならびにディジタル文書へのアクセスの管理を説明する。暗号エンベロープは最新の暗号化技法（暗号化および認証などの）を使用して、文書部分を無許可の読取りや改竄に対して安全なものとする。

【０００７】本明細書で説明するプロセスにより、暗号エンベロープのパーツをユーザが購入し、ユーザの情報内容を安全で管理された態様で公開することが可能となる。パーツをさらに処理して、海賊行為を防止する。さらに、公開キー技法を使用することにより、暗号エンベロープ技法がディジタル情報を配布する便利で、安全で独立した手段となる。

【０００８】スーパー・ディストリビューション
本明細書で想定している情報配布の基本モデルは「スーパー・ディストリビューション」である（これの詳細については、［５］参照）。基本的な考え方は、各ディジタル文書が「暗号化」されている限り、この文書（または、「パーツ」）をインターネットにより、無線またはテレビジョン信号により、ケーブルにより、人工衛星により、ローカル・エリア・ネットワークにより、ディスケットにより、ＣＤ－ＲＯＭにより、ＢＢＳにより自由に配布できるということである。「暗号化プロセスが十分安全なものであるとすると」、ユーザがコンテンツにアクセスできる唯一の方法は、必要なＰＥＫ（パーツ暗号キー：part encryptionkey）を購入することである。このキーは通常、ユーザが暗号解読する文書よりも数桁コンパクトなものである。

【０００９】スーパー・ディストリビューションは情報配布の問題を、（１）バルク・データの配布と、（２）ＰＥＫの公開によるコンテンツの管理された公開とに分割しているため、強力な概念である。

【００１０】本発明はこの基本的な概念を拡張し、コンテンツの配布および販売に暗号エンベロープの技法を導入する。さらに、これらの概念と技法を一般化して、ディジタル文書へのアクセスおよびその使用に関する「契約条件」を取り扱う。一般化することによって、暗号エンベロープをディジタル文書の分散アクセス監理の設計および実施の基礎として使用することが可能となる。

【００１１】本発明はこのようなキー・データベースをサーバに維持することを不必要とし、さらにドキュメント・サーバ（コンテンツが暗号化されるところ）とバイ

・サーバ（文書暗号キーを取得できるところ）とをきれいに分離することを可能とする。
【００１２】したがって、本発明は任意の数のユーザに任意に配布できるが、機密情報パーツの平文テキスト内容にアクセスできるのは許可を受けたユーザだけである暗号エンベロープを作成する方法を提供する。本発明では、情報パーツの各々を対応するパーツ暗号キーによって暗号化して、暗号化情報パーツを生成する。各パーツ暗号キーを次いで、公開キーによって暗号化する。エンベロープに収められたパーツのリストも作成され、リストの各エントリはパーツ名と個々のパーツの機密ハッシュを有している。この場合、エンベロープは暗号化情報パーツ、暗号解読済み情報パーツ、暗号化パーツ暗号キーおよびパーツのリストを含んでいる。さらに、パーツのリストには署名を作成するために秘密キーによって署名がなされる。この署名もエンベロープに収められる。リストの完全性はリストの署名に使用された秘密キーに関連づけられた第２の公開キーを使ってチェックできる。任意の情報パーツの完全性はパーツの第２のハッシュを計算し、第２のハッシュをリスト内のそのパーツの対応するハッシュと比較することによってチェックできる。さらに、暗号化されたパーツの情報コンテンツは開示に対して保護され、これを復元できるのはパーツ暗号キーだけである。公開キーに対応した機密に関する知識は、暗号解読済みのパーツ暗号キーから取得する必要がある。次に、この暗号解読済みパーツ暗号キーが、情報パーツから平文テキストを生成するために使用される。
【００１３】
【発明の実施の形態】図１を参照すると、暗号エンベロープの主要な利点の１つは安全保護である。ＢＳ（バイ・サーバ）１０２およびＤＳ（ドキュメント・サーバ）１００が安全なものとする。たとえば、これらは企業内のそれぞれのビジネス・パートナーによって管理され、所有されており、コンピュータ室内の信頼できる人間によって運用される。
【００１４】また、ＵＰＣ（ユーザのパーソナル・コンピュータ）１０１はユーザに属するものであるから、安全保護がソフトウェアや改竄防止ハードウェアによって与えられる比較的小規模で、安全なＤＦＷＭ（Decryption Fingerprinting and Watermarking Module：暗号解読指紋／透かし付与モジュール）１０３があることを除けば、十分な安全保護がないものとする。
【００１５】ステップの概要処理ステップの概要は以下の通りである（図１参照）。
【００１６】ステップ１。暗号エンベロープの作成
ステップ２。暗号エンベロープの配布
ステップ３。ユーザが行う購入要求
ステップ４。バイ・サーバの応答
ステップ５。暗号エンベロープの開封
【００１７】暗号エンベロープ処理ステップ
これらの処理ステップの各々を以下で詳細に説明する。
【００１８】ステップ１。暗号エンベロープの作成
最初のステップは暗号エンベロープの作成である。図２の２００参照。作成事象はスーパー・ディストリビューションすべきディジタル文書を集める必要があると考えられるため、通常、コンテンツ・プロバイダによってオフラインで行われる。
【００１９】あるいは、これをユーザの要請で開始してもよい。この場合には、暗号エンベロープが特にこのユーザのために作成されることとなり、暗号エンベロープはそのユーザあるいは要請に固有な情報を含んでいてもよい。さらに、他のユーザから将来同様な要請があると予想される場合には、付加的な情報を暗号エンベロープに含め、暗号エンベロープを「キャッシュ」して、将来の類似した要請を効率よく満たすようにすることもできる。
【００２０】暗号エンベロープのパーツ
暗号エンベロープは「情報パーツ」をグループ化したものである。図２の２０１－２１１参照。情報パーツの中には暗号化されたものも、平文テキストのものもある。暗号エンベロープ・プロセスは広範囲にわたるグループ化技術（ｚｉｐ、ｔａｒおよびＯｐｅｎＤｏｃ　Ｂｅｎｔｏやマイクロソフトｏｌｅなどのオブジェクト指向度の高い手法）と両立する。グループ化方法の要件は最小限である。（１）パーツを配布に適したユニットにまとめ、パーツを後で個別に検索できるようにする、（２）さまざまなパーツを、たとえば、命名、ポインタ、あるいは索引などで関連づける手段がなければならない。
【００２１】情報パーツには２つのタイプ、すなわち「ドキュメント」（２０１および２０３）と、「コントロール」（２０２、２０４－２１１）がある。ドキュメント・パーツは「コンテンツ」である。ドキュメント・パーツの例としては、要約、目次、図、表、および本文などがある。これらは、実行可能プログラム、サブルーチン・ライブラリ、ソフトウェア・モジュール、あるいはオブジェクト・コンポーネントの一部となることもできる。
【００２２】図２を参照すると、ドキュメント・パーツは暗号化することができる（２０３）。暗号化ドキュメント・パーツ２０３はユーザが購入する「価値のあるコンテンツ」（たとえば、書物の章、高解像度ＪＰＥＧピクチャ、あるいはＭＰＥＧストリーム）であることがしばしばある。未暗号化パーツは「ティーザ」２０１（たとえば、他人による書評、目次、要約、または低解像度ＪＰＥＧピクチャ）である。未暗号化パーツの目的はユーザがユーザが実際に購入する前に、暗号エンベロープの内容の「プレビュー」、「サンプリング」、または「ブラウズ」を行えるようにすることである。
【００２３】特別なストリング・パターンの圧縮および挿入などの前処理の中には、ドキュメント・パーツに適

用されるものもある。圧縮は記憶域を削減する。他の前処理はＤＦＷＭによるドキュメント・パーツの指紋／透かし付与を容易とするためのドキュメント・パーツに対する改変である。

【００２４】コントロール・パーツは暗号エンベロープの機能およびプロセス・モデルをサポートするのに必要なメタデータである。２つの主要機能、「真性性」と「秘密性」がある。暗号エンベロープでこれらは改竄されない。この認証機能はディジタル署名を使用して達成される。秘密性機能は暗号化（たとえば、ＤＥＳまたはＩＤＥＡを使用した）によって達成される。これらの暗号化および認証技法の基礎となるものは当分野で周知であり、暗号に関する新しいどの文献にも載っている（たとえば、［１］参照）。すべてのコントロール・パーツは認証を受けるし、また、必要に応じて、暗号化されるものもある。

【００２５】コントロール・パーツの例としては価格マトリックス（図４の４００参照）や、ドキュメント・パーツの後処理用の指紋／透かし付与命令２０５がある。ドキュメント・パーツの後処理は、暗号エンベロープが開かれたときに、ＤＦＷＭによって行われる。指紋／透かし付与は後処理の例であり、ドキュメント・パーツに何らかの態様でマークを付けて、海賊行為を防止する。

【００２６】図４を参照する。価格マトリックス４００はドキュメント・パーツの購入に関する価格構造、たとえば、複数部購入時の数量割引、会員割引、または企業割引を記述している。式の例４０１はｎ部の文書の購入価格を計算するものである。（注：価格割引率は時間によって変動するものであってもよく、その場合には、価格マトリックスの列（４０２－４０５）は会員ではなく、期間限定の特別価格となる。）

【００２７】図２を参照すると、ドキュメント・パーツの購入および使用に関する契約条件２０６も暗号エンベロープに含まれている。これらはドキュメント・パーツ（この場合には、ユーザに可視となる）として含まれていても、あるいはコントロール・パーツ（この場合には、バイ・サーバ（ＢＳ）１０２で評価され、またおそらくはユーザのパーソナル・コンピュータ（ＵＰＣ）１０１でも評価される）として含まれていてもよい。ドキュメント・パーツは契約条件を実現する何らかのプログラム（たとえば、Ｐｅｒｌ［４］などのスクリプト言語で書かれた）を含んでいてもよい。（注：指紋／透かし付与命令と価格マトリックス。明確とするため、これらを明示的にリストする。）

【００２８】秘密性および真性性

秘密性を達成することのできる方法をここで説明する。価値の一部はＤＥＳ（データ暗号化規格）アルゴリズム（たとえば、［１］参照）を使用して暗号化される。異なるパーツは異なるＰＥＫ（パーツ暗号化キー）を使用して暗号化される。これらのキーはランダムに、かつ独立して選択される。

【００２９】ランダム暗号化キーを生成するには、多くの方法がある。１つの方法は乱数発生器または疑似乱数発生器を使用して、キーとして使用されるランダム・ストリングを作成することである。この手法の詳細については、［１、３］を参照されたい。

【００３０】各ＰＥＫはＢＳ（バイ・サーバ）１０２の公開キーを使用して暗号化され、得られる暗号化ＰＥＫ２０２（図２）は暗号エンベロープのコントロール・パーツとなる。（注：ＰＥＫを異なるＢＳ公開キーを使用して暗号化することができ、これらすべての暗号化されたＰＥＫは暗号エンベロープに含められる。）

【００３１】暗号エンベロープおよびそのパーツの真性性を確認するには、多くの方法がある。このような方法の１つをここで説明する。すべての暗号エンベロープはＢＯＭ（部品表）２０７という特別なコントロール・パーツを有している。ＢＯＭは２つの部分、（１）パーツ・リスト２０９と（２）ディジタル署名２０８からなっている。

【００３２】機密ハッシュ機能MessageDigest5（ＭＤ５）（詳細については、［１］参照）を、暗号エンベロープに含まれている各パーツに適用し、リストを作成する。図３を参照すると、リストの各エントリはパーツ名すなわち参照３０２と、パーツ名に対応した情報パーツの機密ハッシュ３０１を含んでいる。（たとえば、ファイル・ベースのグループ化の場合、パーツ・リストはすべてのファイルのファイル名とこれらの対応するハッシュ結果を含むものとなる。）

【００３３】次いで、リストにはＤＳ（ドキュメント・サーバ）１００だけにわかる秘密キーによってディジタル署名がされる。文書にディジタル署名を行うには多くの方法がある（たとえば、［１］参照）。１つの方法はパーツ・リストのＭＤ５（または、その他の機密ハッシュ）を計算し、得られるハッシュを秘密キー（「署名」を作成する）２０８を使用して暗号化することである。パーツ・リストおよび署名をまとめてＢＯＭ２０７という。ＢＯＭの真性性を検査するのに必要なのは、ＤＳの公開キーだけである。

【００３４】暗号エンベロープの真性性はＤＳの公開キーを使用して署名を暗号解読し、これをパーツ・リストのＭＤ５と比較することによって調べられる。２つが合致すれば、パーツ・リストは改竄されていないことになる。個々のパーツの真性性も各パーツのＭＤ５を計算し、その結果をリストの対応するエントリと比較することによって調べることができる。したがって、ＢＯＭ２０７は暗号エンベロープとそのすべてのパーツの完全性を保証するものである。

【００３５】独立した暗号エンベロープ

暗号エンベロープの重要な特徴はこれが以下の意味で独立していることである。暗号エンベロープの真性性を検

査するのに必要なのは、ＤＳの公開キーだけである。暗号化ＰＥＫ（２０２、２１０、２１１。図２参照）が暗号エンベロープに付随しているため、内容を復元するのに必要なのは、ＢＳの秘密キーだけである。さらに、異なるドキュメント・サーバはＢＳの公開キーだけを使用して暗号エンベロープを生成することができ、ＢＳとＤＳの間の他の通信は必要ない。

【００３６】暗号エンベロープ作成ステップ

暗号エンベロープの作成時の処理ステップをまとめると、次のようになる（図２参照）。

【００３７】１－ａ。暗号エンベロープに含める情報パーツをアセンブルする。

【００３８】１－ｂ。オプションの処理ステップ（たとえば、圧縮、事前指紋／事前透かし付加）をパーツに適用する。後で操作やり直すため、これらの処理ステップの十分な状態情報を維持しておく。

【００３９】１－ｃ。暗号化対象の各パーツに１つ、ランダムなＰＥＫ（パーツ暗号化キー）を生成する。

【００４０】１－ｄ。ドキュメント・パーツをそれぞれのＰＥＫによって暗号化して、暗号エンベロープに含められる暗号化されたパーツ（２０３、２０４、２０５）を形成する。

【００４１】１－ｅ。次に、ＢＳの公開キーを使用して、ＰＥＫを暗号化して、暗号エンベロープに含められる暗号化ＰＥＫ（２０２、２１０、２１１）を形成する。暗号化ＰＥＫおよびその対応する暗号化パーツは関連づけられる。

【００４２】１－ｆ。また、何らかのランダムＰＥＫを使用して、処理ステップ１－ｂの命令およびその他の状態情報を暗号化する。ＰＥＫはＢＳの公開キーによって暗号化される。暗号化パーツ（２０３、２０４、２０５）および暗号化ＰＥＫ（２０２、２１０、２１１）は両方とも暗号エンベロープに収められる。

【００４３】１－ｇ。暗号エンベロープに、「ティーザ」、概要および目次などの平文テキスト２０１を収める。

【００４４】１－ｈ。指紋／透かし付与命令２０５や価格マトリックス２０６などの契約条件を収める。必要に応じ、パーツやサブパーツを暗号化する（そして、これらの暗号化ＰＥＫを収める）。前述のように、暗号化パーツをその暗号化ＰＥＫと関連づける。

【００４５】１－ｉ。アセンブルしたすべてのパーツをリストし、リストされたパーツの各々に対して機密ハッシュを計算して、情報パーツのリスト２０９を作成する。

【００４６】１－ｊ。リストにディジタル署名を行うことによって、たとえば、リストの機密ハッシュを計算し、これをＤＳ秘密キーによって暗号化することによってＢＯＭ２０７に対する署名２０８を作成する。ＢＯＭ２０７（リスト２０９および署名２０８）を暗号エンベロープに加える。

【００４７】考えられる暗号エンベロープの構造の詳細については、図２を参照されたい。

【００４８】ステップ２。暗号エンベロープの配布

暗号エンベロープが作成されると、これを任意の手段、たとえばインターネットで送信することによって、無線またはテレビジョン信号によって、有線で、人工衛星によって、ＣＤ－ＲＯＭによって、あるいはＢＢＳによって配布することができる。配布の安全保護は必要ない。暗号エンベロープをコピーしたり、複製を作ったり、あるいはユーザ間で共有したりすることができる。実際には、本発明者らが期待しているのは、暗号エンベロープの「下流」での配布（すなわち、友人同士が暗号化エンベロープをコピーすること）が暗号エンベロープを配布する費用効果の高い手段となることである。最後に、暗号エンベロープは任意のサーバの格納することができ、サーバにはいかなるセキュリティ要件もない。

【００４９】ステップ３。ユーザが行う購入要求

このステップは暗号エンベロープの平文の「ティーザ」部分２０１を閲覧したユーザによって行われることがしばしばある。暗号エンベロープの内容に関心を持ったユーザは必要なＰＥＫをＢＳから購入しなければならない（図１参照）。

【００５０】グラフィカル・ユーザ・インタフェース

暗号エンベロープの閲覧は暗号エンベロープの構造を理解している修正ウェブ・ブラウザなどのＧＵＩの助けを借りて行われる。まず、修正ブラウザは暗号エンベロープの完全性を調べる必要がある。ユーザには完全性チェックにより暗号エンベロープの改竄が通知される。次に、ブラウザは暗号エンベロープの平文テキストを表示する、たとえば概要と目次を表示できなければならない。最後に、図２および図５を参照すると、ブラウザは暗号エンベロープ２００から、ＢＲＭ（購入要求メッセージ）５００を構築するのに必要なパーツを抽出できなければならない。

【００５１】事前登録

ユーザがＢＳによって認識されるように、事前登録ステップをユーザが行っているものと想定している。たとえば、ユーザは信頼できるサード・パーティに登録することができる。

【００５２】たとえば、登録はユーザが登録センタに電話をかけ、センタがユーザに対してアカウント番号を発行することを含んでいることができる。アカウント番号は次いで、すべてのＢＳに送られる。あるいは、登録センタはアカウント番号にディジタル署名を行うことができ、この場合には、ＢＳでの更新は必要ない。ＢＳは署名を調べることによってアカウント番号を検査するだけである。

【００５３】登録後、ユーザにはある種の証明書（たとえば、アカウント番号その他の会員情報）が発行され

る。「証明書」は信頼できるサード・パーティがディジタル署名した文書であり、アカウント番号、所属、あるいはユーザが保持している権利などの情報も含んでいる。たとえば、サード・バーティがユーザに対して、表示価格からの割引を受ける権利をユーザに与えるある種の「ブック・クラブ」証明書を発行することができる。

【００５４】機密ＤＦＷＭ

本方法に固有なものとして、登録に結果として、機密ＤＦＷＭ（図１の１０３）（暗号解読指紋透かし付与モジュール）の裏付けがＵＰＣで行われるものと想定していることがある。

【００５５】ＤＦＷＭはパーツの暗号解読を行い、同時に、暗号解読済みパーツに指紋／透かし付与を適用することを担っている。透かし付与は消去が困難であるが、文書の閲読に影響を及ぼさないような態様で、可視のマークを付ける。指紋付与は文書の「不可視」のマークを付けることであり、したがって、除去が困難である。

【００５６】指紋／透かし付与技法の詳細については１９９５年６月２３日出願の米国特許願第０８／４９４６１５号を参照されたい。

【００５７】ＤＦＷＭの裏付け

機密ＤＦＷＭにはさまざまな実施形態がある。最も簡単なものは公開キー技法に基づくものであって、ＤＦＷＭが秘密キーを機密に生成し、これをＤＦＷＭ機密境界内に格納するものである。たとえば、ＤＦＷＭは疑似乱数発生器を使用して、公開秘密キー対を作成することができる。ＤＦＷＭ秘密キーはＤＦＷＭ内に格納され、公開キーは外部に公開される。登録プロセスによって、信頼できるサード・パーティがＤＦＷＭ公開キーを証明することができるようになる（公開キーの証明プロセスについては、［１］参照）。ＤＦＷＭ秘密キーはＤＦＷＭモジュールの唯一の秘密情報である。

【００５８】ＤＦＷＭのセキュリティ

ＤＦＷＭは物理的に安全なモジュール（たとえば、スマート・カード）で動作している、あるいはＵＰＣ環境（安全ではない）で動作しているソフトウェアの一部である。前者の場合、セキュリティはパッケージの物理的改竄防止策によって達成される。現在のパッケージング技術はすべての実用上の目的でＤＦＷＭに十分なセキュリティを与えることができる。

【００５９】後者の場合、すなわち、ＤＦＷＭの物理的セキュリティを想定していない場合に説明を絞る。この場合の方が興味深いのは、物理的セキュリティが利用できることはＤＦＷＭのセキュリティを橋架するだけのものだからである。

【００６０】安全なハードウェアがなければ、ＤＦＷＭのセキュリティを保証することができない。実用上多くの場合に、周知のソフトウェア技法（たとえば、ウィルスの作成者に周知のコード隠滅技法）を使用して、十分なセキュリティを達成できる。

【００６１】しかしながら、本開示で記載するプロセスの主な利点の１つは、ＤＦＷＭが危険にさらされたとしても、エクスポージャが限定されることである。ユーザは購入していないドキュメント・パーツのロックを解除することができない（ＰＥＫを利用できないため）。安全なＢＳを経由するため、購買トランザクションは安全である。

【００６２】ＤＦＷＭが危険にさらされた場合（たとえば、ＤＦＷＭの秘密キーが暴露された場合）、考えられる損失はユーザが購入した文書に正しい指紋／透かし付与を行えないということだけとなる。しかしながら、セキュリティ・リスクはユーザが文書からマークを消去する可能性とまったく異なるというものではない。

【００６３】購入要求トランザクション

ここで、購入要求トランザクションを詳細に説明する。

【００６４】グラフィカル・ユーザ・インタフェース（ＧＵＩ）により、ユーザには暗号エンベロープに収められている物品リストが表示される。ユーザは関連する概要を閲覧して、詳細な情報を得ることができる。ユーザは物品の表示価格を知ることもできる。ユーザが物品の購入を希望する場合には、ＧＵＩによって購入要求を行い、ＢＲＭ（購入要求メッセージ）（図５の５００参照）がＢＳ１０２へ送られることとなる。

【００６５】ユーザの認証

購入要求を完全なものとする前に、システムがユーザの認証を行おうとすることもある。システムによるユーザの認証には多くの周知の方法がある。たとえば、このような技法の１つ（Pretty Good Privacy［３］で使用されているものと類似したもの）は、暗号化されたユーザの秘密キーをＵＰＣのディスク装置に格納するものである。

【００６６】ユーザはそのパスワードを入力するよう要求され、パスワードは秘密キーを暗号解読するために使用される。秘密キーはディジタル署名を行うか、あるいは購入関係のメッセージを確認するために使用され、各セッションの終了時に消去される。

【００６７】環境変数

環境変数はユーザの環境に関する情報、またはＵＰＣに関する情報（たとえば、場所、時間、機械タイプ、オペレーティング・システム名など）である。これとは対照的に、ユーザ証明書はユーザに関する情報である。

【００６８】環境変数には２つのタイプ、すなわち「安全」および「非安全」がある。安全変数は検証され、ディジタル署名される。これらをＢＳにより（登録中に）調べ、署名するか、あるいはＤＦＷＭによって生成して、署名するかのいずれかを行うことができる。

【００６９】非安全変数はＵＰＣによって生成される。これらは検証されず、また署名されない。これらは情報のためにのみ含められる。本明細書全体にわたり、環境変数とはこれら両者を意味するものとする。

【００７０】購入要求メッセージ
図５を参照すると、ＢＲＭ５００は暗号エンベロープ（図２の２００）からコピーまたは抽出した次の情報を含んでいる。
【００７１】３．１　暗号エンベロープ２０７のＢＯＭ
【００７２】３．２　購入する物品リスト５０１
【００７３】３．３　物品リストおよびその他の制御パーツ（２０２および２１１）に関連づけられたＰＥＫ
【００７４】３．４　契約条件（価格マトリックスなど）２０６
【００７５】また、ユーザ環境またはＤＦＷＭから、あるいはユーザがコピーまたは抽出した次の情報を含んでいる。
【００７６】３．５　ユーザ証明書のリスト（たとえば、会員カードや割引カード）およびユーザ認証関連情報５０２
【００７７】３．６　環境変数（たとえば、日時、場所、ＤＦＷＭまたは機械のハードウェアＩＤ）５０３
【００７８】３．７　ＤＦＷＭ公開キー５０４
【００７９】暗号化および認証などの標準的な暗号技法をＢＲＭに適用することもできる。ＢＲＭを認証する方法の１つはＢＲＭ全体のＭＤ５を計算し、ＤＦＷＭの秘密キーを使用して、得られるＭＤ５を暗号化して、署名５０５を作成し、署名をＢＲＭの末尾に追加することである。
【００８０】ＢＲＭの生成までのステップをまとめると次のようになる。
【００８１】３－ａ。ＧＵＩによる暗号エンベロープの平文部分の閲読。
【００８２】３－ｂ。購入する暗号エンベロープの情報パーツの選択。
【００８３】３－ｃ。購入契約条件２０６（たとえば、表示価格、再販しない約束）に対するユーザによる明示的な同意。
【００８４】３－ｄ。認証のためのパスワードの入力のユーザに対する要求（その結果、ある種のユーザ認証関連情報が生成され、ＢＲＭに含められる）。
【００８５】３－ｅ。ＧＵＩによるＢＲＭ５００の生成。
【００８６】３－ｆ。ＢＳへのＢＲＭの送信。
【００８７】注：ＢＲＭを特別なタイプの暗号エンベロープ、すなわち「購入要求」暗号エンベロープと見なすことができる。
【００８８】ステップ４。バイ・サーバの応答
ＢＳＲ（バイ・サーバ応答）はＢＲＭを受信すると送られる。ＢＳＲの送信前にＢＳ（バイ・サーバ）が行う動作を詳細に説明する。
【００８９】ユーザ口座
ＢＳはＢＲＭを受信すると、ＢＯＭを検証して、コントロール・パーツの真性性を調べる。また、ＤＦＷＭ公開キー、ユーザ証明書、およびユーザ認証関連情報の真性性も調べる。ユーザは以前の登録ステップによりＢＳに口座を持っていることがあり、その場合には、該当する金額がユーザの口座から引き落とされる（ユーザが権利を持っている割引を適用した後）。
【００９０】契約条件の評価
暗号エンベロープ（および、ＢＲＭに）に収められている契約条件２０６の主な目的は、購買を成立されるのに必要な、契約条件に記載されている要件をユーザが満たしていることを確認することである。ＢＳは契約条件を評価（実行）することによって、ユーザが要件を満たしていることを調べる。評価の結果により、購買を完了できるかどうかが判定される。結果が満足できるものであれば、他のステップが継続され、そうでない場合には、エラー・メッセージがＢＳＲに入れられる。結果が満足できるものである場合、実購入価格も価格マトリックス（４００）で与えられた式４０１を使用して計算される。
【００９１】キーの変換
ＢＲＭでＢＳが行う動作の１つはキーの変換である。ステップ１で述べたように、ＰＥＫ（パーツ暗号化キー）はＢＳの公開キーを使用して暗号化されている。ＢＳはその秘密キーを使用してＰＥＫを暗号解読する。暗号化ＰＥＫの暗号解読後、ＢＳはＤＦＷＭの公開キーを使用して、ＰＥＫを再暗号化し、ＤＦＷＭだけがＰＥＫを復元できるようにする。これがキー変換ステップである。
【００９２】指紋／透かし付与のカスタム化
ＢＳが行う他の一連の動作は指紋／透かし付与命令のカスタム化である。ステップ１で述べたように、これらの命令はＢＳ公開キーを使用して暗号化され、コントロール・パーツとして暗号エンベロープで搬送される。ＢＳはまず命令を暗号解読し、次に、ユーザに関する情報（たとえば、ユーザ名、会員番号）およびトランザクションに関する情報（たとえば、購入日、ライセンスの限定事項、トランザクションＩＤ）を命令に含める。これらの命令は次いで、ＤＦＷＭ公開キーを使用して暗号化される。（ＤＦＷＭはこれらの暗号化された指紋／透かし付与命令が存在していることを調べてから、文書を暗号解読する。）
【００９３】契約条件の変換
コンテンツの使用に関する制限事項に関する他の態様が、ＢＳＲに含められる。ＢＲＭに収められている契約条件が強化されたり、修正されたりすることがある（たとえば、暗号エンベロープが作成されてから、契約条件が変更される）。結果として生じる契約条件は文書の使用に関する制限事項および契約条件を記載した簡単な平文テキストとなる。あるいは、契約条件を守らせる実行可能な命令、オブジェクト、およびエージェントであってもよい。これらはすべてＢＳＲに収められている。
【００９４】購入応答ステップ

図６を参照して、ＢＲＭの受信からＢＳＲの送信までにＢＳが行うステップをまとめる。
【００９５】４－ａ。ＢＲＭの受信
【００９６】４－ｂ。ＢＲＭの真性性を調べ（ＢＯＭを調べることにより）、ユーザの証明書を検証し、ユーザの認証関連情報を検証し、ＤＦＷＭ公開キーを検証し、環境変数を調べる。
【００９７】４－ｃ。ユーザの証明書、価格マトリックス、および環境変数を入力（ＢＲＭからの）として、またデータベースにあるユーザ情報および付加的な環境変数を入力（ＢＳからの）として使用して、契約条件を評価する。契約条件の評価からの出力は、（ａ）ユーザがパーツのアクセスすることを認められているかどうか、および（ｂ）パーツ６０１を購入する実際の価格となる。
【００９８】４－ｄ。ユーザにアクセスが認められているかどうか、またユーザに十分な信用があるかどうかを調べる。そうでない場合には、異常終了し、エラーＢＳＲを送信する。
【００９９】４－ｅ。ＰＥＫを変換する（ＢＳ秘密キーを使用してＰＥＫを暗号解読し、ＤＦＷＭ公開キーを使用してＰＥＫを再暗号化する）。これらをＢＳＲに含める（６０２、６０３）。
【０１００】４－ｆ。指紋／透かし付与命令をカスタム化する。（命令を暗号解読し、ユーザ固有のトランザクション関連情報を命令に含める。ＤＦＷＭ公開キーを使用して、修正された命令を暗号化する。）これらをＢＳＲに含める（６０４）。
【０１０１】４－ｇ。文書の使用に関する変換された契約条件およびその他の制限事項をＢＳＲに含める（６０５）。
【０１０２】４－ｈ。ＢＳＲをユーザに送る。
【０１０３】ＢＳＲを特別なタイプの暗号エンベロープ、すなわち「ライセンス暗号エンベロープ」と見なすことができる。この場合も、暗号化および認証などの標準的な暗号技法を適用して、ＢＳＲのプライバシーと真性性を保護することができる（６０６）（たとえば、［１］参照）。
【０１０４】ステップ５。暗号エンベロープの開封
これは最終ステップである。このステップの前提条件は、ＢＳからＢＳＲを受け取っていることである。ＢＳＲの受信後、ユーザは都合のよいときに暗号エンベロープを開くことができる。
【０１０５】ＢＳＲは暗号エンベロープのロックを解除する「キー」である。ＰＥＫがすべてＤＦＷＭ公開キーで暗号化されているため、ＢＳＲの内容を使用できるのは「特定」のＤＦＷＭだけである。図６を参照すると、暗号エンベロープの開封に関与するステップは次のようになる。
【０１０６】５－ａ。ＤＦＷＭがＢＳＲの真性性を確認するため、チェックを行う（６０６）。開封作業が継続されるのは、ＢＳＲの認証が成功した場合だけである。
【０１０７】５－ｂ。ユーザに対して任意選択で、更新された契約条件６０５をＢＳＲで求める。開封作業が継続されるのは、ユーザが契約条件に同意した場合だけである。
【０１０８】５－ｃ。ＤＦＷＭが変換されたＰＥＫ（６０２、６０３）とカスタム化された指紋／透かし付与命令（６０４）を認証し、暗号解読する。開封作業が継続されるのは、認証が成功した場合だけである。
【０１０９】５－ｄ。暗号解読したＰＥＫを使用して、ＤＦＷＭが暗号エンベロープの対応する暗号化されたパーツを暗号解読する（２０３、２０５）。
【０１１０】５－ｅ。ＤＦＷＭが該当する指紋／透かし付与命令６０４を暗号解読した文書に適用する。（指紋／透かし付与はユーザに合わせてカスタム化され、無許可の配布をさらに防止する。）
【０１１１】５－ｆ。得られる暗号解読された文書が、ＤＦＷＭセキュリティ境界外のユーザに対して許可される。
【０１１２】暗号エンベロープのプロセスを、一般にきわめて機密性が高いデータ（患者の医療記録など）やデータベースに対して効率がよく、安全な分散アクセス管理を実施するために使用することもできる。
【０１１３】参照文献
１．B. Schneier, "Applied Cryptography, 2nd Edition," Addison Wesley, 1996。
２．ＩＢＭ　ＣＤ－Ｓｈｏｗｃａｓｅ特許（１９９４年６月７日にＢ．Ｈａｌｔｅｒ他に対して発行された米国特許第５３１９７０５号）。
３．S. Garfinkel, "Pretty Good Privacy," O'Reilly &; Associates, Inc., 1994。
４．L. W. WallおよびR. L. Schwartz, "Programming Perl," O'Reilly &; Associates, Inc., 1991。
５．B. Cox, "Superdistribution and Electronic Objects," Dr. Dobb's Journal, Vol. 17, No. 10, Oct. 1992。
６．本出願人に譲渡された１９９５年６月２３日出願の米国特許願第０８／４９４６１５号「A METHOD TO DETER DOCUMENT AND INTELLECTUAL PROPERTY PRIVACYTHROUGH INDIVIDUALIZATION」。
参照文献［１－６］は参照することにより、本明細書の一部となる。
【０１１４】まとめとして、本発明の構成に関して以下の事項を開示する。
【０１１５】（１）複数のユーザに任意に配布でき、情報パーツの集合体であるディジタル文書である暗号エンベロープを作成する方法において、
ａ．前記情報パーツの１つをパーツ暗号化キーによって暗号化して、前記エンベロープに収められる暗号化パー

ツを作成するステップと、
ｂ．前記パーツ暗号化キーを第１の公開キーによって暗号化して、前記暗号エンベロープに収められる暗号化パーツ暗号化キーを作成するステップと、
ｃ．前記エンベロープに収められているパーツのリストであって、該リストの各エントリがパーツ名と該命名パーツの機密ハッシュとを含んでおり、該リストも前記エンベロープに収められるパーツのリストを作成するステップと、
ｄ．前記リストに第１の秘密キーによって署名して、前記エンベロープに収められる署名を作成するステップとを備えており、前記リストの完全性を前記第１の秘密キーに関連づけられた第２の公開キーによって調べて、前記署名を検証することができ、前記エンベロープのいずれか１つのパーツの完全性を該１つのパーツの第２の機密ハッシュを計算し、かつ該第２のハッシュを前記リスト内の対応するハッシュと比較することによって調べることができ、前記暗号エンベロープの情報コンテンツが開示から保護され、前記パーツ暗号化キーによってのみ復元することができ、前記パーツ暗号化キーが前記第１の公開キーに対応する第２の秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読することによってのみ復元できる、暗号エンベロープを作成する方法。
（２）前記文書の前記パーツから選択したものを、この選択したパーツ内の選択したワードまたはビットの挿入、削除または変更により修正し、それぞれの未修正の文書を復元するために、修正した各ドキュメント・パーツをその修正に関連づける状態情報を維持するステップをさらに含んでいる、上記（１）に記載の方法。
（３）前記パーツの前記暗号化前に、前記修正を前記パーツから選択したものに適用し、第３の公開キーによって暗号化される第３のパーツ暗号化キーを使用して、前記状態情報を暗号化する、上記（２）に記載の方法。
（４）前記暗号エンベロープが、サーバで実行されるものであるコンピュータ・プログラムを含んでおり、前記実行の結果が前記サーバによる以降の操作を決定する、上記（１）に記載の方法。
（５）前記プログラムが前記暗号エンベロープ内の前記情報パーツのアクセスに関する契約条件を記述しており、前記実行が前記情報パーツへのアクセスが許可されるかどうかを決定する、上記（４）に記載の方法。
（６）前記プログラムが各情報パーツを修正する命令を含んでおり、各パーツが各パーツ内の選択したワードまたはビットの挿入、削除、または変更によって修正され、それぞれの未修正の文書を復元するために、修正した各ドキュメント・パーツをその修正に関連づける状態情報が維持される、上記（４）に記載の方法。
（７）暗号エンベロープ内のコンテンツ・データへのアクセスをもたらす方法において、
ａ．前記暗号エンベロープのパーツへのアクセス要求であり、前記パーツを暗号化するために使用されたキーの公開キー暗号化である暗号化パーツ暗号化キーを少なくとも含んでいる要求をユーザからのサーバに伝送するステップと、
ｂ．前記要求に応じて、前記サーバから前記ユーザへ、前記暗号化パーツ暗号化キーの変形物である応答を伝送するステップとを備えており、前記変形物が前記公開キーに関連づけられた秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読し、第２の公開キーを使用して前記パーツ暗号化キーを暗号化し、前記変形化キーを前記秘密キーを使用して、前記パーツ暗号化キーに暗号解読することによって生成され、前記の選択したパーツが前記パーツ暗号化キーを使用して平文テキストに暗号解読され、これによって前記ユーザにアクセスを与える前記方法。
（８）複数の端末装置へ電子的にアクセスするサーバを有する通信ネットワークにおいて、選択したコンテンツ・データへのアクセスを与える方法において、前記暗号エンベロープが
ａ．複数のユーザに任意に配布でき、情報パーツの集合体であるディジタル文書である暗号エンベロープを作成することによって生成され、該生成方法が（ｉ）その１つが前記の選択したコンテンツ・データを含んでいる、保護されるべき前記パーツの各々にパーツ暗号化キーを関連づけ、（ｉｉ）保護されるべき前記パーツの各々をこれに関連したパーツ暗号化キーによって暗号化し、
（ｉｉｉ）前記の各パーツ暗号化キーを公開キーによって暗号化して、前記パーツ暗号化キーの各々に対する暗号化パーツ暗号化キーを形成し、（ｉｖ）各エントリが前記パーツの１つに対するパーツ名と該１つのパーツに対する機密ハッシュとを含んでいるパーツのリストを作成し、（ｖ）前記リストに秘密キーによって署名して、署名を作成することからなっており、前記暗号エンベロープが前記署名、前記リスト、前記暗号化パーツ暗号化キー、前記暗号化パーツ、および前記情報パーツのうち暗号化されていないものの集合体であり、
ｂ．前記暗号エンベロープのコピーを所有しているユーザが前記の選択したコンテンツ・データにアクセスすることを希望した場合に、（ｉ）前記暗号エンベロープの前記の選択したコンテンツ・データを含んでいるパーツへのアクセス要求であり、前記パーツを暗号化するために使用されたキーの公開キー暗号化である暗号化パーツ暗号化キーを少なくとも含んでいる要求を前記ユーザからサーバへ伝送し、（ｉｉ）前記要求に応じて、前記サーバから前記ユーザへ、前記暗号化パーツ暗号化キーの変形物である応答を伝送することによって前記アクセスが与えられ、前記変形物がステップｂ（ｉ）の前記公開キーに関連づけられた秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読し、第２の公開キーを使用して前記要求の前記パーツ暗号化キーを暗号化し、前記変

形化キーを前記秘密キーを使用して、前記要求の前記パーツ暗号化キーに暗号解読することによって生成され、前記の選択したパーツが前記パーツ暗号化キーを使用して平文テキストに暗号解読され、これによって前記ユーザにアクセスを与える前記方法。

【図面の簡単な説明】

【図１】暗号エンベロープ・プロセスの５つのステップの概要を示す図であり、このプロセスに関与する主なエントリがドキュメント・サーバ（ＤＳ）１００、バイ・サーバ（ＢＳ）１０２、暗号解読指紋／透かし付与モジュール（ＤＦＷＭ）１０３、およびユーザのパーソナル・コンピュータ（ＵＰＣ）１０１であることを示す図である。

【図２】典型的な暗号エンベロープの構造を示す図であり、最小限の要素が暗号化パーツ２０３、ならびにこれに関連した暗号化パーツ暗号キー（ＰＥＫ）２０２、パーツ・リスト２０９、およびパーツ・リストの署名２０８であることを示す図である。

【図３】パーツ・リスト２０９を有する部品表（ＢＯＭ）の構造を示す図である。表の各エントリはパーツ名３０２（たとえば、「Abstract」）、および個々のパーツのMessageDigest5（ＭＤ５）、すなわち機密ハッシュ３０１（たとえば、「13ADBF77F...」）とを含んでいる。リストのＭＤ５が計算され、得られるハッシュにはＤＳの秘密キーを使用して署名がされ、ディジタル署名２０８が作成される。リスト２０９および署名２０８がＢＯＭを形成する。

【図４】典型的な価格マトリックスを示す図である。列はさまざまな会員カテゴリ（４０２、４０３、４０４、４０５）に対する割引率を示し、行は数量割引（４０６、４０７、４０８、４０９）を示す。ｎ部目の価格とｎ部の合計価格を計算する式の例は４０１に示すとおりである。

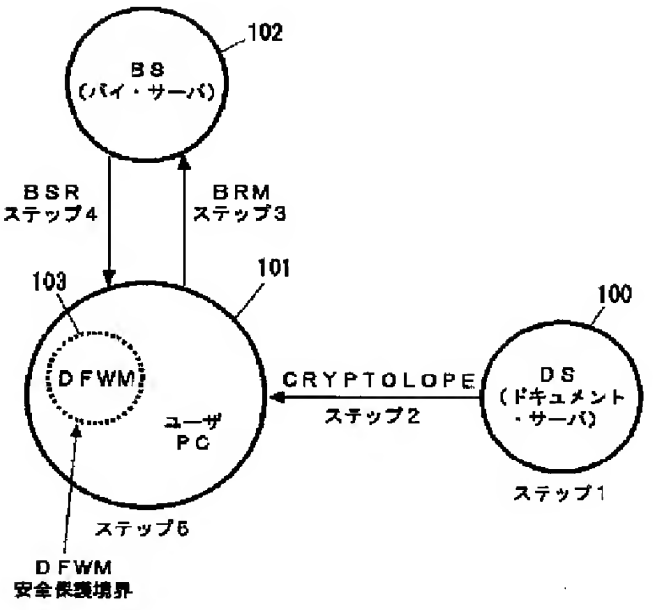
【図５】購入要求メッセージ（ＢＲＭ）５００を示す図である。ＢＲＭには、暗号化ＰＥＫ（２０２、２１１）、暗号化指紋／透かし付与命令２０５、契約条件２０６、およびＢＯＭ２０７が含まれる。項目２０２、２０５、２０６、２０７および２１１は暗号エンベロープ２００（図２参照）からコピーされる。ＢＲＭの他の部分（５０１－５０５）はＵＰＣで生成される。

【図６】バイ・サーバ応答（ＢＳＲ）６００を示す。バイ・サーバ（ＢＳ）はＰＥＫを変換して、ＤＦＷＭ１０３だけが暗号解読できる変換ＰＥＫ（６０２、６０３）を作成する。指紋／透かし付与命令は暗号解読、カストマイズ、および再暗号化され、その結果６０４を暗号解読できるのはＤＦＷＭだけとなる。ＢＲＭ（５００、図５）にある契約条件も評価され、更新または変換された契約条件６０５を作成する。実購入価格６０１は該当する割引を基本価格に適用することによって計算される。

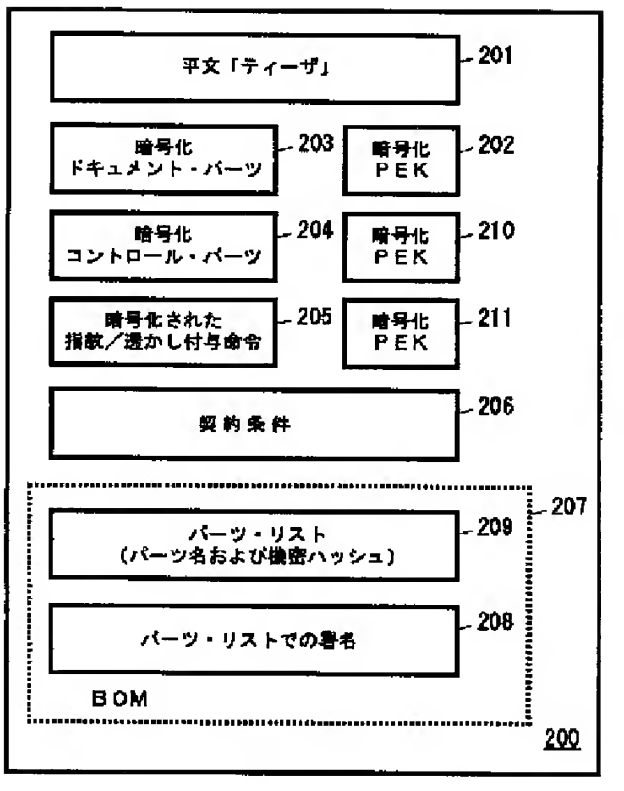
【符号の説明】

１００　ドキュメント・サーバ（ＤＳ）
１０１　ユーザのパーソナル・コンピュータ（ＵＰＣ）
１０２　バイ・サーバ（ＢＳ）
１０３　暗号解読指紋／透かし付与モジュール（ＤＦＷＭ）

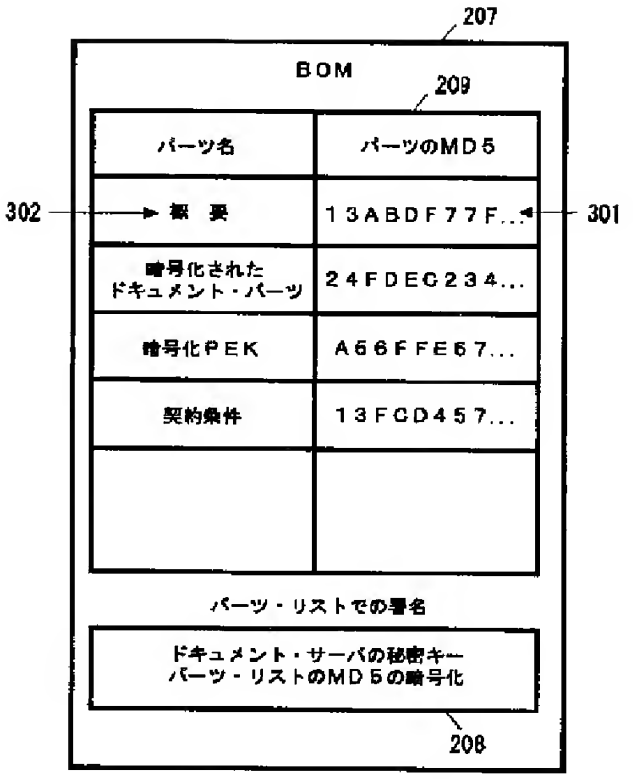
【図１】



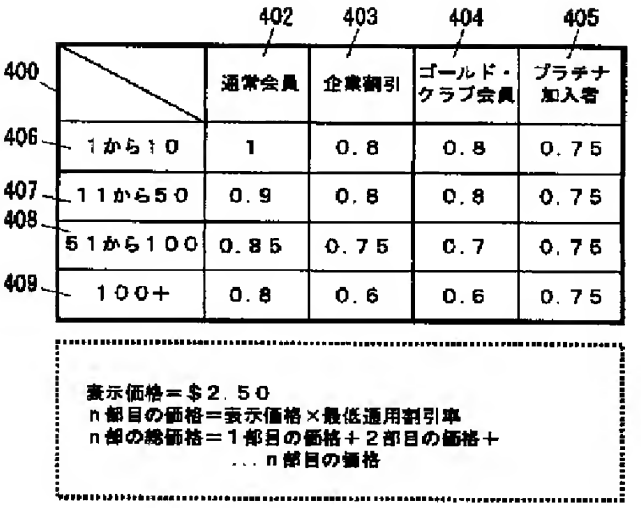

【図２】



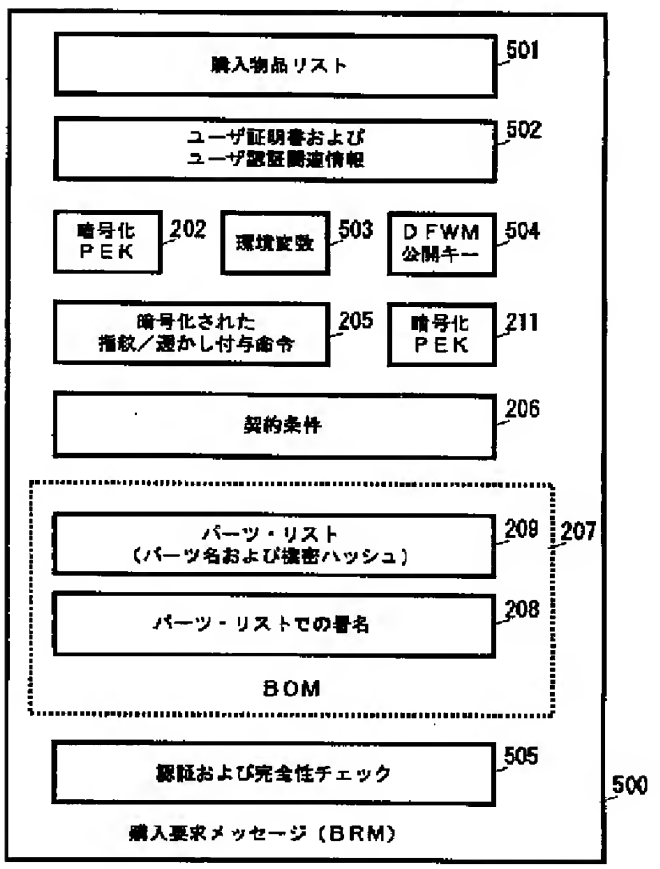
【図３】


207
BOM
209
パーツ名
パーツのMD５
302
概　要
１３ＡＢＤＦ７７Ｆ...
301
暗号化された
ドキュメント・パーツ
２４ＦＤＥＣ２３４...
暗号化ＰＥＫ
Ａ６６ＦＦＥ６７...
契約条件
１３ＦＣＤ４５７...
パーツ・リストでの署名
ドキュメント・サーバの秘密キー
パーツ・リストのＭＤ５の暗号化
208

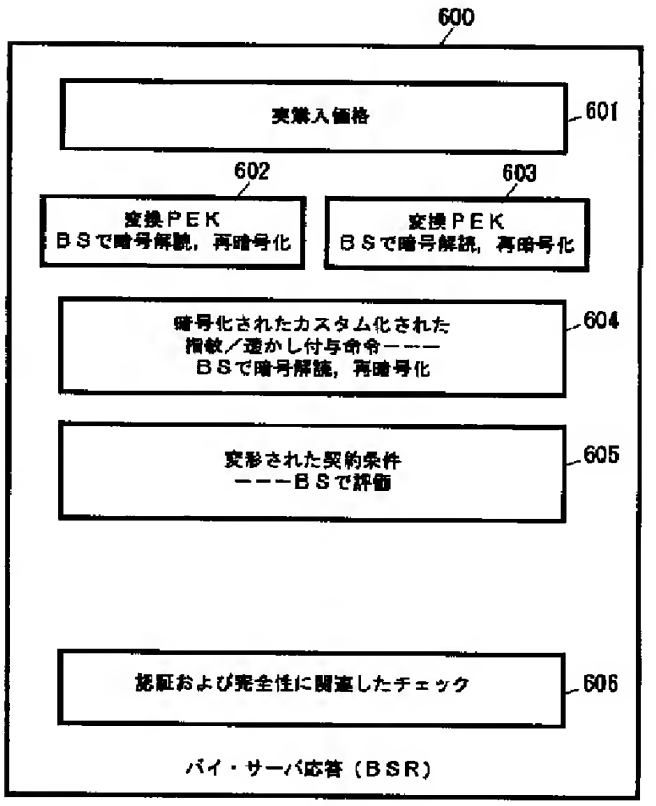
【図４】


400
402
403
404
405
通常会員
企業割引
ゴールド・
クラブ会員
プラチナ
加入者
406
１から１０
１
０．８
０．８
０．７５
407
１１から５０
０．９
０．８
０．８
０．７５
408
５１から１００
０．８５
０．７５
０．７
０．７５
409
１００＋
０．８
０．６
０．６
０．７５
表示価格＝＄２．５０
ｎ部目の価格＝表示価格×最低適用割引率
ｎ部の総価格＝１部目の価格＋２部目の価格＋
...ｎ部目の価格

【図５】


購入物品リスト
501
ユーザ証明書および
ユーザ認証関連情報
502
暗号化
ＰＥＫ
202
環境変数
503
ＤＦＷＭ
公開キー
504
暗号化された
指紋／透かし付与命令
205
暗号化
ＰＥＫ
211
契約条件
206
パーツ・リスト
（パーツ名および機密ハッシュ）
209
207
パーツ・リストでの署名
208
ＢＯＭ
認証および完全性チェック
505
500
購入要求メッセージ（ＢＲＭ）

【図６】


600
実購入価格
601
602
603
変換ＰＥＫ
ＢＳで暗号解読，再暗号化
変換ＰＥＫ
ＢＳで暗号解読，再暗号化
暗号化されたカスタム化された
指紋／透かし付与命令－－－
ＢＳで暗号解読，再暗号化
604
変形された契約条件
－－－ＢＳで評価
605
認証および完全性に関連したチェック
606
バイ・サーバ応答（ＢＳＲ）

フロントページの続き

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|
| Ｈ０４Ｌ | 9/08 | | Ｈ０４Ｌ | 9/00 | ６０１Ａ |
| | 9/14 | | | | ６４１ |

(72)発明者　チー＝セン・チョウ
アメリカ合衆国95014　カリフォルニア州
クパチーノ　メイグス・レーン　19030

(72)発明者　マーク・アダム・カプラン
アメリカ合衆国10536　ニューヨーク州カ
トナーホーリー・ヒル・レーン　14

(72)発明者　ジェフリー・チャールズ・クリグラー
アメリカ合衆国　バージニア州マクリーン
ディキシー・プレース　8601